4. (Canceled)

5. (Currently amended) The apparatus of claim [[5]]1, wherein the encrypted password comprises a unique password configured to be decrypted by the cryptographic module that first created the encrypted password.

6. (Original) The apparatus of claim 1, wherein the computer readable medium module further comprises a backup utility module configured to selectively copy data from a storage device source, detect newer versions of data stored on the storage device source, and replace older versions of the data on the computer readable medium with newer versions of the data.

fem 12/27/07

7. (Previously Presented) A device for secure computer readable medium backup, the device comprising:

a motherboard;

a cryptographic module coupled to the motherboard and configured to communicate with a computer readable medium; and

the computer readable medium comprising a trusted platform interface module configured to communicate with the cryptographic module, wherein the trusted platform interface module comprises a password module, the trusted platform interface module initializing the password module in response to verifying the cryptographic module by comparing a known value stored on the password module to a cryptographic module platform configuration register value storing a hash of POST BIOS code, wherein only the cryptographic module may initialize the password module, the password module configured to store and transmit an encrypted password to the cryptographic module, and receive an unencrypted password from the cryptographic module.